UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

ELECTRONIC PRIVACY INFORMATION CENTER, et al.,

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT, et al.,

Defendants.

Civil No. 1:25-cv-255-RDA-WBP

MEMORANDUM OF LAW
IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Defendants U.S. Office of Personnel Management ("OPM"); Charles Ezell, in his official capacity as Acting Director of OPM; U.S. Department of the Treasury ("Treasury"); Scott Bessent, in his official capacity as Secretary of the Treasury; the U.S. Digital Service, redesignated as the U.S. Department of Government Efficiency Service, or U.S. DOGE Service ("USDS"); the Acting U.S. Digital Service Administrator; and the U.S. DOGE Service Temporary Organization, submit this Memorandum in Support of their Motion to Dismiss Plaintiffs' Complaint (ECF No. 1).

INTRODUCTION

This case rests on Plaintiffs' fear of hypothetical consequences that might—or might not—result from certain federal employees being given access to Treasury and OPM's data systems. But granting employees access to agency data systems is a routine governmental decision made daily across any number of government agencies, and Plaintiffs' speculation about hypothetical consequences cannot serve as the basis for a federal action. Indeed, well established law forecloses Plaintiffs' attempt to have this Court oversee the day-to-day information-technology operations of Treasury and OPM. Plaintiffs lack standing even to bring this action because the hypothetical future harms they allege in their Complaint do not constitute a cognizable injury in fact. And even if this Court had subject-matter jurisdiction, Plaintiffs fail to plead a plausible claim for relief under the Administrative Procedure Act, the Privacy Act, the Internal Revenue Code, the Fifth Amendment, or an ultra vires agency action theory. The Court should therefore grant Defendants' motion and dismiss this action.

BACKGROUND

I. The United States Department of Government Efficiency Service

On January 20, 2025, President Trump signed Executive Order 14,158, which directs changes to the previously established U.S. Digital Service designed to implement the President's agenda of "improv[ing] the quality and efficiency of government-wide software, network

infrastructure, and information technology (IT) systems." 90 Fed. Reg. 8,441, § 4 ("USDS EO"). The USDS EO also redesignated the U.S. Digital Service as the Department of Government Efficiency Service, or U.S. DOGE Service ("USDS"). *Id.* § 3(a). It established a "U.S. DOGE Service Temporary Organization" in the Executive Office of the President under 5 U.S.C. § 3161, which will terminate on July 4, 2026. USDS EO § 3(b). The USDS EO requires agency heads to establish in their respective agencies a USDS team of at least four employees. *Id.* § 3(c).

The USDS EO directs USDS to collaborate with Executive agencies to "modernize" the technology and software infrastructure of the federal government to "improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems" as well as "ensure data integrity." USDS EO § 4. To accomplish its objectives, the USDS EO directs USDS to work with relevant agency heads, and vice versa, to ensure USDS has access to "unclassified agency records, software systems, and IT systems" to the "extent consistent with law." *Id.* § 4(b). At all times, the USDS EO instructs, USDS must "adhere to rigorous data protection standards." *Id*.

Executive Order 14,170, also issued on January 20, 2025, tasks the Director of OPM, among others, with developing a Federal Hiring Plan that, among other things, "integrate[s] modern technology to support the recruitment and selection process, including the use of data analytics to identify trends, gaps, and opportunities in hiring." 90 Fed. Reg. 8,621, § 2(b)(vi).

II. Plaintiffs' Complaint

A. Plaintiffs allege that Treasury and OPM have granted access to their systems to "USDS/DOGE Personnel"

Plaintiffs filed this suit on February 10, 2025. Compl. (ECF No. 1). Plaintiffs are the Electronic Privacy Information Center ("EPIC"), a nonprofit organization, and Doe 1, a current federal agency employee. Compl. ¶¶ 9-10. The Complaint alleges that simply by granting access

to "USDS/DOGE Personnel" as directed by the USDS EO, Treasury and OPM have "disclosed vast stores of personal information contained in" the agencies' Bureau of the Fiscal Service ("BFS") and Enterprise Human Resources Integration ("EHRI"), respectively. *Id*. ¶¶ 32, 38, 57, 77, 86. According to the Complaint, by granting that access to their systems, Treasury and OPM have "unlawfully disclos[ed] extremely personal information about Plaintiffs . . . to unchecked actors in violation of law." *Id*. ¶ 96. Neither EPIC, on behalf of any individual member, nor Doe allege in the Complaint that this alleged access was to *their* information as opposed to the BFS and EHRI systems generally or that any information at all was disclosed to non-government recipients. *See generally id*.

B. Plaintiffs' claims and requests for relief

The Complaint asserts five causes of action. In Count One, Plaintiffs allege that Treasury and OPM's conduct is arbitrary, capricious, an abuse of discretion, or otherwise contrary to law under the Administrative Procedure Act, 5 U.S.C. § 706(2)(A), because Treasury and OPM have administered systems "without complying with statutorily required security protections under" the Federal Information Security Modernization Act of 2014 ("FISMA"), 44 U.S.C. §§ 3554(a)(1)-(2). Compl. ¶¶ 105-09. In Count Two, Plaintiffs allege that Treasury and OPM have violated the Privacy Act of 1974 by "disclos[ing]" Plaintiffs' personal data in violation of 5 U.S.C. § 552a(b) and by "us[ing] such data for computer matching" in violation of § 552a(o). *Id*. ¶¶ 110-12. In Count Three, Plaintiff Doe 1, only, alleges that Treasury and USDS, but not OPM, have "disclos[ed] and inspect[ed]" her tax return information in violation of the Internal Revenue Code, 26 U.S.C. § 6103. *Id*. ¶¶ 113-18. In Count Four, Plaintiffs claim that Defendants, "by providing access to confidential personal information," have deprived EPIC's members and Doe 1 of their liberty interest in "avoiding disclosure of personal matters" under the Fifth Amendment's Due Process Clause. *Id*. ¶¶ 119-22. And in Count Five, Plaintiffs assert a mandamus claim, alleging

that the "DOGE Defendants" have engaged in ultra vires actions "[i]n directing and controlling the use and administration" of the BFS and EHRI systems without legal authority. *Id*. ¶¶ 123-128.

III. Procedural history

On February 12, Plaintiffs filed a motion for a temporary restraining order. *See* Mot. (ECF No. 5). The motion was fully briefed, *see* ECF Nos. 7, 19, 20, and the Court held argument on February 21, *see* ECF No. 32. The Court converted the motion into one for a preliminary injunction and denied it the same day. *See* Feb. 21, 2025 Mem. Op. and Order (ECF No. 35).

STANDARD OF REVIEW

I. Rule 12(b)(1)

Rule 12(b)(1) allows a party to move to dismiss a complaint for lack of subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). "A challenge to subject matter jurisdiction under Rule 12(b)(1) may be facial or factual. A facial challenge contends that the complaint fails to allege facts upon which subject matter jurisdiction can be based. In reviewing a facial challenge, "all the facts alleged in the complaint are assumed to be true and the plaintiff . . . is afforded the same procedural protection as he would receive under a Rule 12(b)(6) consideration." *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). In either a facial or factual challenge, "the plaintiff bears the burden of proving jurisdiction." *Bradford v. Mattis*, No. 3:18-CV-570-HEH, 2018 WL 6834360, at *2 (E.D. Va. Dec. 28, 2018) (citations omitted).

II. Rule 12(b)(6)

To survive a motion to dismiss under Rule 12(b)(6), a complaint "must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A complaint must provide "more than labels and conclusions" because "a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint's legal claims must be supported by factual

allegations that "raise a right to relief above the speculative level." *Id*. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678. The plausibility standard requires more than a showing of "a sheer possibility that a defendant has acted unlawfully." *Id*. Instead, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*.

ARGUMENT

Plaintiffs lack standing, and thus the Court lacks jurisdiction, because they do not allege a concrete injury in fact. Even if they had standing, Plaintiffs' claims each fail to state a claim because, as a matter of law, the agency-database access they allege does not violate the APA, the Privacy Act, the Internal Revenue Code, or any Fifth Amendment privacy right, and is not ultra vires agency action. Plaintiffs' Complaint should be dismissed.

I. Plaintiffs lack Article III standing because they have not alleged a cognizable injury in fact.

The Complaint should be dismissed under Rule 12(b)(1) because both EPIC and Doe fail to carry their burden to plead standing. To establish standing, "a plaintiff must demonstrate (i) that she has suffered or likely will suffer an injury in fact, (ii) that the injury likely was caused or will be caused by the defendant, and (iii) that the injury likely would be redressed by the requested judicial relief." *Food & Drug Admin. v. Alliance for Hippocratic Med.*, 602 U.S. 367, 380 (2024) (citations omitted). "Those specific standing requirements constitute an essential and unchanging part of the case-or-controversy requirement of Article III." *Id*. (internal quotation marks and citations omitted). "'When the plaintiff is not himself the object of the government action or inaction he challenges, standing is not precluded, but it is ordinarily 'substantially more difficult' to establish.'" *N. Va. Hemp & Agric., LLC v. Virginia*, 125 F.4th 472, 489 (4th Cir. 2025) (quoting

Summers v. Earth Island Inst., 555 U.S. 488, 493-94 (2009)). And "[t]he party seeking to establish standing carries the burden of demonstrating these elements." *Chambers Med. Techs. of S.C., Inc. v. Bryant*, 52 F.3d 1252, 1265 (4th Cir. 1995).

EPIC, for its members,[1] and Doe have not demonstrated that they have suffered any injury in fact. To satisfy Article III standing, harm must be "actual or imminent, not speculative," meaning "the injury must have already occurred or be likely to occur soon." *Alliance for Hippocratic Med.*, 602 U.S. at 381. The harm must also be "concrete." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021). To be concrete, an injury in fact must have a "close relationship" to a "harm traditionally recognized as providing a basis for a lawsuit in American courts." *Id*. at 417, 424 (quotation omitted). That inquiry asks whether "plaintiffs have identified a close historical or common-law analogue for their asserted injury." *Id.* at 424. Concrete intangible harms include injuries such as "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* at 425. An alleged statutory violation alone does not meet that standard because "Article III standing requires a concrete injury even in the context of a statutory violation." *Id*. at 426 (internal quotation marks and citation removed).

Those requirements are fatal to Plaintiffs here. Plaintiffs assert a purely intangible form of injury—they allege that Treasury and OPM's granting access to USDS-affiliated personnel constitutes an invasion of privacy. *See, e.g.*, Compl. ¶¶ 96, 120. That injury is not concrete.

[1] As an organization, EPIC "can demonstrate Article III standing either in [its] own right or as a representative of [its] members." *Maryland Election Integrity, LLC v. Maryland State Bd. of Elections*, 127 F.4th 534, 538 (4th Cir. 2025) (internal quotation marks and citation omitted). EPIC does not rely on alleged injury to the organization itself but instead to the privacy interests of its members. Compl. ¶ 120. "To establish representational standing," EPIC "must demonstrate that" its "members would otherwise have standing to sue in their own right." *Maryland Election Integrity, LLC*, 127 F.4th at 538 (internal quotation marks and citation omitted). To do so, EPIC must establish injury in fact as to those members. *Id*.

Plaintiffs do not contend their information has been shared with parties outside the government. The USDS employees at the relevant agencies are bound by the same legal and ethical restrictions on the disclosure of Plaintiffs' information that bind all agency employees with access to that information. USDS EO § 4(b). As in *TransUnion*, 594 U.S. at 434, the mere fact that Treasury and OPM allegedly committed a statutory violation in allowing government employees to access government databases that store information does not alone demonstrate a concrete harm.

Nor have Plaintiffs "identified a close historical or common-law analogue for their asserted injury." *TransUnion*, 594 U.S. at 424. The Complaint identifies none. *See generally* Compl. To the extent Plaintiffs rely on the tort of intrusion upon seclusion, *see* Pls.' Reply in Supp. Mot. (ECF No. 20) at 6-9, that does not suffice. That tort "is the intentional intrusion, 'physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person.'" *Elec. Priv. Info. Ctr. v. U.S. Off. of Pers. Mgmt.*, No. 1:25-CV-255 (RDA/WBP), 2025 WL 580596, at *5 (E.D. Va. Feb. 21, 2025) (quoting Restatement (Second) of Torts, § 652B (Am. L. Inst. 1977)). But as the Fourth Circuit held just last week in staying, pending appeal, the district court's preliminary injunction in *American Federation of Teachers v. Bessent*—another challenge to USDS teams' access to agency record systems—the alleged "abstract access to personal information" does not establish a concrete injury analogous to the tort of intrusion upon seclusion because Plaintiffs here, like appellees there, "fail to allege any interjection into the private sphere analogous to the unsolicited mailings in *Garey* [*v. James S. Farrin. P.C.*, 35 F.4th 917 (4th Cir. 2022)] or the unsolicited phone calls in *Krakauer* [*v. Dish Network*, 925 F.3d 643 (4th Cir. 2019)]." No. 25-1282, 2025 WL 1023638, at *2 (4th Cir. Apr. 7, 2025) (Agee, J., concurring). "At its core, the harm contemplated by the common-law tort of intrusion upon seclusion includes an intrusion into an individual's private space." *Id.*; *see*

O'Leary v. TrustedID, Inc., 60 F.4th 240, 246 (4th Cir. 2023) ("It's the unwanted intrusion into the home that marks intrusion upon seclusion, and [plaintiff] hasn't pleaded anything that closely relates to that."). Treasury and OPM granting access to federal government employees to Treasury and OPM databases that store individuals' personal information does not bear a "close relationship" to an intrusion into private space. As the Fourth Circuit found, "more than abstract access to personal information" is necessary "to establish a concrete injury." 2025 WL 1023638, at *2. Because Plaintiffs fail to plead a cognizable injury in fact, they lack standing, and the Court should dismiss their Complaint.

II. Plaintiffs' claims each should be dismissed under Rule 12(b)(6) for failure to state a claim, even had they sufficiently pleaded standing.

A. Plaintiffs have not pleaded a cognizable APA claim (Count I).

1) An agency's FISMA implementation is not subject to judicial review.

Plaintiffs allege that Defendants violated the Administrative Procedure Act, 5 U.S.C. § 706(2)(A), by "administer[ing] systems . . . without complying with" the requirements of the Federal Information Systems Modernization Act" ("FISMA"). Compl. ¶¶ 106-07. Plaintiffs' APA claim fails because a federal agency's FISMA compliance is committed to agency discretion and is therefore not judicially reviewable.

The APA explicitly excludes from judicial review those agency actions that are "committed to agency discretion by law." 5 U.S.C. § 701(a)(2). To determine whether a matter has been committed to agency discretion, the Fourth Circuit applies a two-part inquiry. *Holbrook v. Tennessee Valley Auth.*, 48 F.4th 282, 290 (4th Cir. 2022). First, the Court asks whether the agency action "is the kind of agency action that has traditionally been committed to agency discretion." *Id*. (internal quotation marks and citations omitted). If so, the Court must then determine whether

the relevant statute "intentionally limits agency discretion by setting guidelines or otherwise providing a limit" for agency discretion. *Id*.

Here, as to the first part, Congress passed FISMA to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3551(1). Congress, however, specifically "recognize[d] that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products." 44 U.S.C.A. § 3551(6). In the FISMA context, then, agency action is expressly "the kind of agency action . . . committed to agency discretion." *Holbrook*, 48 F.4th at 290.

As to the second part—any limit to that discretion—FISMA offers no specific prescriptions for the tools or methods required, which is unsurprising considering the rapidly evolving nature of both technology and cyber threats. Instead, Congress vested agencies with broad discretion to adopt "security protections commensurate with the risk and magnitude of the harm" resulting from cyber threats. 44 U.S.C. § 3554(a)(1)(A). FISMA gives agencies latitude to develop security policies and procedures that are "appropriate" and "cost-effectively reduce information security risks to an acceptable level." *Id*. at § 3554(b)(2)(B). To achieve its goals, FISMA assigns *exclusive* responsibility for overseeing the management and security of information systems of civilian agencies to the Director of the Office of Management and Budget ("OMB"). FISMA mandates that the OMB Director "shall oversee agency information security policies and practices, including . . . overseeing agency compliance with the requirements of this subchapter [of FISMA.]" *Id*. § 3553(a)(5). FISMA specifically authorizes the OMB Director "to enforce accountability for compliance," *id.*, through various mechanisms, including by "tak[ing] any action that the Director considers appropriate, including an action involving the budgetary process or appropriations

management process," 40 U.S.C. § 11303(b)(5)(A). The Director also must review each agency's security programs at least annually and approve or disapprove them. 44 U.S.C. § 3553(a)(5). Finally, he must report to Congress annually on the "effectiveness of information security policies and practices during the preceding year." *Id.* § 3553(c). Accordingly, a federal agency's compliance with FISMA is committed to agency discretion by law, and FISMA cannot be the basis of Plaintiffs' APA claim. *See Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006) ("Notably absent from FISMA is a role for the judicial branch. We are far from certain that courts would ever be able to review the choices an agency makes in carrying out its FISMA obligations."); *Am. Fed'n of Lab. & Cong. of Indus. Organizations v. Dep't of Lab.*, No. CV 25-0339 (JDB), 2025 WL 542825, at *4 (D.D.C. Feb. 14, 2025) ("Plaintiffs' arguments that defendants are violating . . . FISMA . . . are not likely to succeed because FISMA may not be subject to review under the APA." (citing *Cobell*, 455 F.3d at 314)); *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 266 F. Supp. 3d 1, 44 (D.D.C. 2017), *aff'd in part, rev'd in part in other grounds and remanded*, 928 F.3d 42 (D.C. Cir. 2019) ("The Court holds that OPM's actions in carrying out [FISMA's] requirements is committed to the agency's discretion, and not subject to judicial review under the APA.").

2) The agency database access alleged here is not agency action that is subject to APA review.

Plaintiffs' APA claim also fails because they do not challenge discrete Treasury or OPM action; rather, they attack the agencies' programmatic activities that are not agency action subject to APA review. "When challenging agency action . . . the plaintiff must . . . identify specific and discrete governmental conduct, rather than launch a broad programmatic attack on the government's operations." *City of New York v. U.S. Dep't of Def.*, 913 F.3d 423, 431 (4th Cir. 2019) (internal quotation marks and citation omitted). And "[r]eview is available only when acts are discrete in character, required by law, and bear on a party's rights and obligations." *Id*. at 432.

Plaintiffs challenge Treasury and OPM's database-access practices in general in effectuating Executive Order 14,158; they do not identify, for instance, a specific unauthorized disclosure. *See generally* Compl. Plaintiffs thus "ask that [the Court] supervise an agency's compliance with the broad statutory mandate of [FISMA]." *City of New York*, 913 F.3d at 433 (internal quotation marks and citation omitted). That compliance "is the sort of public policy problem that often requires reallocating resources, developing new administrative systems, . . . working closely with partners across government[, and] will likely require expertise in information technology and deep knowledge of how [Treasury and OPM] needs intersect with data collection." *Id*. It is "exactly the sort of 'broad programmatic' undertaking for which the APA has foreclosed judicial review." *Id*. (quoting *Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 64 (2004) ("*SUWA*") (quoting 5 U.S.C. § 704)).

3) Even if Plaintiffs had identified judicially reviewable agency action, they have not identified a final agency action.

Even if Plaintiffs had identified judicially reviewable agency action, their APA claim fails because they have not identified a *final* agency action. APA review is limited to "final agency action." *SUWA*, 542 U.S. at 61-62 (quoting 5 U.S.C. § 704). Agency action is final only when it "mark[s] the consummation of the agency's decisionmaking process" and is "one by which rights or obligations have been determined, or from which legal consequences will flow." *U.S. Army Corps of Eng'rs v. Hawkes Co., Inc.*, 578 U.S. 590, 597 (2016) (quoting *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997)). The APA does not permit "general judicial review of [an agency's] day-to-day operations." *Lujan v. National Wildlife Fed'n*, 497 U.S. 871, 899 (1990). Nor does the APA authorize courts to oversee "the common business of managing government programs." *Fund for Animals, Inc. v. U.S. Bur. of Land Mgmt.*, 460 F.3d 13, 20 (D.C. Cir. 2006).

Plaintiffs' Complaint fails to show how providing federal employees with system access necessary to carry out a lawfully issued Executive Order creates any rights, obligations, or legal consequences for Plaintiffs. *Sierra Club v. EPA*, 955 F.3d 56, 63 (D.C. Cir. 2020) (no agency action where the challenged act "impose[d] no obligations, prohibitions or restrictions on regulated entities," and "d[id] not subject them to new penalties or enforcement risks"). Instead, Plaintiffs' Complaint seeks review of day-to-day management of agency operations. Indeed, the alleged "agency action" Plaintiffs identify is a series of personnel decisions related to granting government employees access to agency data systems. These are precisely the type of day-to-day operational decisions that the Supreme Court in *Lujan* advised do not fall within the APA's ambit. *See Lujan*, 497 U.S. at 899. And it is the kind of APA challenge where "courts would be forced either to enter a disfavored 'obey the law' injunction or to engage in day-to-day oversight of the executive's administrative practices. Both alternatives are foreclosed by the APA, and rightly so." *City of New York*, 913 F.3d at (citations omitted); *Am. Fed'n of Teachers*, 2025 WL 1023638, at *5 (Richardson, J., concurring) ("The agency action here—granting IT access to certain employees—does not fit comfortably into either bucket [of the two-pronged final-agency-action test].").

4) Plaintiffs' APA claims are barred because they have an adequate, alternative remedy

Plaintiffs' APA claims fail for the additional, independent reason that the APA cause of action exists only when "there is no other adequate remedy in a court." 5 U.S.C. § 704; *Bowen v. Massachusetts*, 487 U.S. 879, 903 (1988) (Section 704 "makes it clear that Congress did not intend the general grant of review in the APA to duplicate existing procedures for review of agency action."). That is not the case here. The Privacy Act provides a "comprehensive remedial scheme" for injuries arising out of the inappropriate dissemination of private information about individuals. *Wilson v. Libby*, 535 F.3d 697, 703 (D.C. Cir. 2008) (citing *Chung v. Dep't of Justice*, 333 F.3d

273, 274 (D.C. Cir. 2003)). And the other-adequate-remedy bar applies even where the plaintiff may not succeed on the merits of her claim under the alternative statutory review procedure; the existence of that procedure alone suffices. *See Rimmer v. Holder*, 700 F.3d 246, 261-62 (6th Cir. 2012); *Jones v. U.S. Dep't of Hous. & Urban Dev.*, No. 11 CIV. 0846 (RJD) (JMA), 2012 WL 1940845, at *6 (E.D.N.Y. May 29, 2012) (reasoning that an alternative was adequate "whether or not relief is ultimately granted"). Plaintiffs' APA claim should be dismissed. *But see Am. Fed'n of Teachers v. Bessent*, No. CV DLB-25-0430, 2025 WL 895326, at *19 n.17 (D. Md. Mar. 24, 2025); *Am. Fed'n of Gov't Emps., AFL-CIO v. U.S. Off. of Pers. Mgmt.*, No. 25CV1237 (DLC), 2025 WL 996542, at *18 (S.D.N.Y. Apr. 3, 2025).

B. Plaintiffs' have not alleged a violation of the Privacy Act (Count II).

1) Plaintiffs do not allege "disclosure" of information about Doe or EPIC's members.

The Privacy Act limits the ability of an "agency" to "disclose" any "record" that is "contained in a system of records . . . to any person, or to another agency." 5 U.S.C. § 552a(b). The Privacy Act does not define "disclose." Its ordinary meaning is "[t]o make (something) known or public; to show (something) after a period of inaccessibility or of being unknown; to reveal." Black's Law Dictionary (12th ed. 2024). The Act defines a "record" as "any item, collection, or grouping of information *about an individual* that is maintained by an agency." 5 U.S.C. § 552a(a)(4) (emphasis added).

The Complaint nowhere alleges that information *about Doe or EPIC's members* has been made known, shown, or revealed anywhere; Plaintiffs instead allege only that Treasury and OPM have provided access to systems that *contain* Plaintiffs' records. Even construing "disclose" to mean the mere granting of access, *see Am. Fed'n of Teachers*, 2025 WL 895326, at *19; *Am. Fed'n*

of Gov't Emps., AFL-CIO, 2025 WL 996542, at *12,[2] nowhere does the Complaint allege USDS employees were granted access to "information about [Doe or EPIC members]," 5 U.S.C. § 552a(a)(4)—at most, Plaintiffs allege that USDS employees have merely been granted access to large databases that contain such information somewhere.

2) Section § 552a(b) permits the intra-agency-disclosure for official duties.

Even if the agency-database-access were a Privacy Act disclosure, Plaintiffs' claim fails. The Privacy Act authorizes disclosure of such records to "those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). The access granted to USDS team members within the agencies falls comfortably within that.

As an initial matter, Plaintiffs' allegations that Treasury and OPM "disclos[ed] vast stores of personal information to individuals unauthorized by law to access them, including but not limited to USDS/DOGE personnel," Compl. ¶ 40, ignores that the USDS EO requires agency heads to establish in their respective agencies a USDS team of at least four employees. USDS EO § 3(c). And those agency USDS team members have a "need" to access the records contained in the relevant systems in order to perform their official duties. 5 U.S.C. § 552a(b)(1). The USDS teams at Treasury and OPM exist under the USDS EO to modernize technology and to "[m]aximize [e]fficiency and [p]roductivity." USDS EO § 4. To that end, the USDS EO instructs agency heads "to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems," and in turn requires USDS to

[2] *But see*, *e.g.*, *Luster v. Vilsack*, 667 F.3d 1089, 1098 (10th Cir. 2011); *Walia v. Chertoff*, 2008 WL 5246014, at *11 (E.D.N.Y. Dec. 17, 2008); *Schmidt v. U.S. Dep't of Veterans Affairs*, 218 F.R.D. 619, 630 (E.D. Wis. 2003); *Mittleman v. U.S. Dep't of Treasury*, 919 F. Supp. 461, 468 (D.D.C. 1995).

"adhere to rigorous data protection standards." *Id.* § 4(b). Given the purpose of the USDS EO—to modernize technology—it necessarily follows that agency personnel seeking to improve agency data systems would need access to them to conduct that modernization. Put another way, it would be impossible for the USDS team members to perform the mandated task of modernizing these data systems without access to the systems themselves.

Even if not all disclosures to USDS personnel are considered intra-agency disclosures, Defendants' actions are permissible under the Privacy Act's exception for "routine use." *See* 5 U.S.C. § 552a(b)(3) (permitting disclosure absent consent for certain "Routine Uses" that are defined in a published Systems of Record Notice ("SORN")). Treasury's published Routine Use 17 permits disclosure to federal agency personnel "for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, federal funds." 85 Fed. Reg. 11,776, 11,780 (2020). Treasury's DOGE Team is tasked with doing just that. *See* USDS EO §§ 1, 4. And OPM's SORNs generally permit disclosures to personnel for work on a contract, service, grant, cooperative agreement or job for the federal government. 77 Fed. Reg. 73,694, 73,697 (Dec. 11, 2012).

3) The Complaint alleges no cognizable Privacy Act relief.

Last, the Privacy Act cause of action exists for two categories of claims, neither of which Plaintiffs allege here. First, the Act creates a cause of action for actual money damages when an alleged disclosure has been "intentional or willful." 5 U.S.C. § 552a(g)(4). Because there has been no Privacy Act "disclosure" of Doe's or EPIC's members' records, as set forth above, Plaintiffs do not allege intent or willfulness, which requires "more than gross negligence," *Reinbold v. Evers*, 187 F.3d 348, 361 n.14 (4th Cir. 1999).

Second, the Privacy Act provides for injunctive relief in only two narrow circumstances: (1) to order an agency to amend inaccurate, incomplete, irrelevant, or untimely records, 5 U.S.C.

§ 552a(g)(1)(A), (g)(2)(A); and (2) to order an agency to allow an individual access to his records, *id.* § 552a(g)(1)(B), (g)(3)(A). When, as here, "[a] 'statute provides certain types of equitable relief but not others, it is not proper to imply a broad right to injunctive relief.'" *Parks v. IRS*, 618 F.2d 677, 84 (10th Cir. 1980) (citation omitted). Accordingly, injunctive relief is not available for any other type of Privacy Act claim. *See Sussman v. U.S. Marshal Serv.*, 494 F.3d 1106, 1122 (D.C. Cir. 2007) ("We have held that only monetary damages, not declaratory or injunctive relief, are available to § 552a(g)(1)(D) plaintiffs.") (citing *Doe v. Stephens*, 851 F.2d 1457, 1463 (D.C. Cir. 1988)).

C. Plaintiffs have not alleged a violation of the Internal Revenue Code § 6103 (Count III).

Plaintiffs do not state a claim under § 6103 of the Internal Revenue Code ("IRC"). As an initial matter, only Doe asserts this claim and only with respect to Treasury; Doe does not assert that OPM's data was improperly accessed or disclosed in violation of § 6103. *See* Compl. ¶¶ 114-15, 118. Doe's § 6103 claim fails for the same reason that her Privacy Act claim does. Section 6103 states that no federal employee "shall disclose" tax return information unless otherwise permitted. 26 U.S.C. § 6103(a). As set forth above, Doe does not allege that Treasury has wrongfully inspected or disclosed *her* tax return or return information, just that Treasury has granted access to agency databases that contain tax return information somewhere.

Doe also fails to allege other elements of her claim. "Section 7431 provides a civil cause of action for violations of § 6103." *McKenzie-El v. Internal Revenue Serv.*, No. CV ELH-19-1956, 2020 WL 902546, at *12 (D. Md. Feb. 24, 2020). So to plead her cause of action, Doe must allege that the United States violated § 6103. *See* 26 U.S.C. § 7431(a)(1) ("If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer

may bring a civil action for damages."). And to do that, she "must specifically allege who made the alleged disclosures, to whom they were made, the nature of the disclosures, the circumstances surrounding them, and the dates on which they were made." *Bancroft Global Dev. v. United States*, 330 F. Supp. 3d 82, 101 (D.D.C. 2018) (internal quotation marks omitted); *McKenzie-El*, 2020 WL 902546, at *13 ("To state a claim under § 7431(a), a plaintiff must adequately plead (1) that the disclosure was unauthorized, (2) that the disclosure was made knowingly or by reason of negligence and (3) that the disclosure was in violation of Section 6103. This standard requires that a plaintiff 'specifically allege who made the alleged disclosures, to whom they were made, the nature of the disclosures, the circumstances surrounding them, and the dates on which they were made.'") (first internal quotation marks and citation omitted) (quoting *Bancroft Global Dev.*, 330 F. Supp. 3d at 101). The purpose of this requirement is "to put the Government on notice of which exact actions a plaintiff challenges" so that the defendant "is able to identify which exception, if any, the disclosure will fall into under § 6103" because "[a]bsent a proper identification of the alleged illegally disclosed information, there would be a constant guessing game as to the disclosures and exceptions." *Bancroft Global Dev.*, 330 F. Supp. 3d at 101 (quotation marks and citation omitted). This standard also prevents a plaintiff from proceeding based on the mere speculation that her personal information might have been disclosed or inspected. *McKenzie-El*, 2020 WL 902546, at *13 ("[A] 'plaintiff must also plead what specific return or return information an employee of the United States disclosed that violated § 6103.'") (quoting *Bancroft Global Dev.*, 330 F. Supp. 3d at 101); *see also, e.g.*, *Fostvedt v. I.R.S.*, 824 F. Supp. 978, 985-86 (D. Colo 1993), *aff'd sub nom. Fostvedt v. United States*, 16 F.3d 416 (10th Cir. 1994) (dismissing complaint where plaintiff alleged that IRS special agent made various disclosures unknown to plaintiff).

Doe has not sufficiently alleged a § 6103 violation. The alleged § 6103 violation is that Treasury has "disclos[ed] and inspect[ed] confidential return information contained in the BFS system." Compl. ¶ 116. But even assuming that Treasury granting access to agency databases that contain tax return information somewhere qualifies as a § 6103 disclosure (it does not), Doe does not allege that Treasury has wrongfully inspected or disclosed *her* tax return or return information and thus cannot plead a claim. 26 U.S.C. § 7431(a)(1) ("return or return information *with respect to a taxpayer* . . . *such taxpayer* may bring a civil action"). And in any event, the Complaint does not "specifically allege who made the alleged disclosures, to whom they were made, the nature of the disclosures, the circumstances surrounding them, and the dates on which they were made." *McKenzie-El*, 2020 WL 902546, at *13.

Even if she had alleged a specific unlawful disclosure, Doe's claim would still fail because an exception to the general rule of § 6103(a) applies. "[O]fficers and employees of the Department of the Treasury" may obtain returns and return information if their "official duties require such inspection or disclosure for tax administration purposes." 26 U.S.C. § 6103(h)(1). "Tax administration," in turn, is broadly defined to include "the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws." *Id.* § 6103(b)(4)(A)(i). The payment systems at issue in this case disburse the vast majority of government payments, including tax refunds. *See* Fiscal Service Overview, *available at* https://www.fiscal.treasury.gov/about.html (last visited Apr. 15, 2025). Professionals who maintain and improve the payment systems need access to the data in those systems in order to administer the

tax laws. The USDS team at Treasury satisfied these statutory conditions for access to returns and return information pursuant to the USDS EO.[3]

D. Plaintiffs have not alleged a Fifth Amendment violation (Count IV).

For at least three independent reasons, the Court should dismiss Plaintiffs' claim that Defendants' challenged actions infringe on their claimed due process right to "informational privacy" under the Fifth Amendment.

1. As a threshold matter, the Supreme Court has never held that a constitutional right to informational privacy exists. In the few decisions considering such claims, the Court has merely assumed, without holding, that there is such a right in the course of concluding that the challenged government action did not violate it. *See, e.g.*, *NASA v. Nelson*, 562 U.S. 134, 144-48 (2011). Despite this nonchalance, the Fourth Circuit has recognized an "individual interest in avoiding disclosure of personal matters," albeit one limited to "information with respect to which the individual has a reasonable expectation of privacy." *Payne v. Taslimi*, 998 F.3d 648, 655 (4th Cir. 2021) (quoting *Walls v. City of Petersburg*, 895 F.2d 188, 192-93 (4th Cir. 1990), *abrogated in other part by Lawrence v. Texas*, 539 U.S. 558 (2003)).[4]

Leaving to one side the questionable provenance of the right Plaintiffs claim, to the extent that it exists, it is quite narrow. The Supreme Court and the Fourth Circuit have considered

[3] Although Plaintiffs assert that access to Treasury's data systems has been provided to non-Treasury employees, all such allegations are entirely conclusory and thus should not be credited on a motion to dismiss. The only well-pleaded allegations concerning access to Treasury's systems, even accounting for the news articles the Complaint appears to incorporate by reference, are that access has been provided to *Treasury employees*. *See, e.g.*, Compl. ¶¶ 35, 38 n.11, 42 n.12, 55 n.38. That would be consistent with the USDS EO, which instructs agencies to create USDS teams comprised of agency "employees." USDS EO § 3(c).

[4] Although *Payne* was constrained to follow *Walls*, the Fourth Circuit made a point of noting the unstable foundation of the claimed right to informational privacy. *See* 998 F.3d at 653-57; *see also Am. Fed'n of Gov't Emps. v. HUD*, 118 F.3d 786, 788 (D.C. Cir. 1997) (expressing "grave doubts" that a right to informational privacy exists).

informational privacy only in the context of (1) the government's *collection* of information (*i.e.*, whether the government may compel individuals to disclose information in the first instance), and (2) the government's *public* disclosure of information within its control (*i.e.*, whether the government may disseminate information it has obtained to third parties). *E.g.*, *Nelson*, 562 U.S. at 138 (employment background investigation); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 429 (1977) (compelled production of former President's papers and tape recordings); *Whalen v. Roe*, 429 U.S. 589, 591 (1977) (compilation of prescriptions for certain drugs); *Payne*, 998 F.3d at 652-53 (doctor's disclosure of prisoner's HIV-positive status); *Walls*, 895 F.2d at 189 (employment questionnaire). And even in those cases, both courts have concluded that the government action either did not implicate or did not violate whatever right to informational privacy there might be.

Defendants have not found a case, and Plaintiffs point to none, involving the distinct question, posed by this case, of whether a government's *internal* sharing of information it already possesses implicates a constitutional informational-privacy right. To the extent that there is any authority on this question, it seems to cut the other way. *See In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 74 (D.C. Cir. 2019) ("[A]ssuming (without deciding) the existence of a constitutional right to informational privacy, it affords relief only for intentional disclosures or their functional equivalent." (internal citations omitted)). In such an "uncharted area" as this, where "guideposts for responsible decision-making . . . are scarce and open-ended," the Court "must be 'reluctant to expand the concept of substantive due process.'" *Hawkins v. Freeman*, 195 F.3d 732, 738 (4th Cir. 1999) (quoting *Washington v. Glucksburg*, 521 U.S. 702, 720 (1997)).

2. Even if Plaintiffs could demonstrate that a right to informational privacy exists *and* that intra-governmental sharing of information implicates the right, Plaintiffs' claim would still fail because the Supreme Court has made clear that "a 'statutory or regulatory duty to avoid

unwarranted disclosures' generally allays . . . privacy concerns." *Nelson*, 562 U.S. at 155 (quoting *Whalen*, 429 U.S. at 605). As relevant here, the requirements of the Privacy Act and the IRC "give 'forceful recognition' to a Government employee's interest in maintaining the 'confidentiality of sensitive information . . . in his personnel files." *Id.* at 156 (quoting *Detroit Edison Co. v. NLRB*, 440 U.S. 301, 318 n.16 (1979)). The Privacy Act and the IRC therefore "'evidence a proper concern' for individual privacy" and obviate any constitutional question regarding individuals' informational privacy. *Id.* (quoting *Whalen*, 429 U.S. at 605).

3. Finally, on top of the fatal defects above, Plaintiffs cannot show that the challenged Executive actions rise to the egregious level required to make out a due process claim. "An executive act can violate substantive due process only when the act shocks the conscience." *United States v. Al-Hamdi*, 356 F.3d 564, 574 (4th Cir. 2004). And "[u]sually," intent to harm is "necessary to satisfy the shocks-the-conscience test for a substantive due process violation." *Slaughter v. Mayor & City Council of Baltimore*, 682 F.3d 317, 320 (4th Cir. 2012) (citing *Cnty. of Sacramento v. Lewis*, 523 U.S. 833, 849 (1998)).

Nothing of the sort occurred here. Treasury and OPM have merely provided federal employees access to digital systems that contain Plaintiffs' personal information. Notwithstanding Plaintiffs' protestations that *these particular* federal employees should not be able to access Plaintiffs' information, and their speculation that such access may make that information more vulnerable to a hypothetical future breach, something so quotidian as intra-governmental information-sharing cannot colorably be classed among "the most egregious official conduct." *Id.* at 321 (quoting *Lewis*, 523 U.S. at 846). Because Plaintiffs cannot show that Defendants "*intended to harm*" them, they cannot establish "conscience-shocking conduct . . . as would be necessary to establish a substantive due process violation." *Id.* at 322.

E. Plaintiffs' ultra vires claim should be dismissed (Count V).

Plaintiffs' ultra vires claim fails. "[C]ourts have recognized that an implicit and narrow exception to the bar on judicial review exists for claims that the agency exceeded the scope of its delegated authority or violated a clear statutory mandate. This exception was first recognized in *Leedom v. Kyne*, 358 U.S. 184 (1958)." *Hanauer v. Reich*, 82 F.3d 1304, 1307 (4th Cir. 1996) (citation omitted). To invoke the *Leedom* exception, a plaintiff "must make (1) a strong and clear demonstration that a clear, specific and mandatory statutory provision has been violated, and (2) the absence of federal court jurisdiction over an agency action would wholly deprive the aggrieved party of a meaningful and adequate means of vindicating its statutory rights." *Scottsdale Cap. Advisors Corp. v. Fin. Indus. Regul. Auth., Inc.*, 844 F.3d 414, 421 (4th Cir. 2016) (cleaned up). A court's "review under the ultra vires standard is necessarily narrow." *Ancient Coin Collectors Guild v. U.S. Customs & Border Prot.*, 698 F.3d 171, 179 (4th Cir. 2012). "Government action is ultra vires if the agency or other government entity is not doing the business which the sovereign has empowered him to do or he is doing it in a way which the sovereign has forbidden." *Id*. (quotation marks and citation omitted). And in applying the *Leedom* exception, courts "may not dictate how government goes about its business but only whether a public entity has acted within the bounds of its authority or overstepped them." *Id*. (quotation marks and citation omitted).

Plaintiffs' ultra vires claim is duplicative of their APA, Privacy Act, IRC, and Fifth Amendment claims. *See* Compl. ¶¶ 124, 127. For all of the reasons those claims fail, as set forth above, Plaintiffs have likewise failed to allege ultra vires action. *But see Am. Fed'n of Gov't Emps., AFL-CIO*, 2025 WL 996542, at *19-20.

CONCLUSION

The Court should dismiss Plaintiffs' Complaint.

Dated: April 15, 2025

Respectfully submitted,

ERIK S. SIEBERT
UNITED STATES ATTORNEY

By: /s/ Jonathan T. Lucier
JONATHAN T. LUCIER, VSB No. 81303
Office of the United States Attorney
919 East Main Street, Suite 1900
Richmond, Virginia 23219
Tel.: (804) 819-5400
Fax: (804) 771-2316
Email: jonathan.lucier@usdoj.gov

PETER B. BAUMHART
Office of the United States Attorney
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel.: (703) 299-3738
Fax: (703) 299-3983
Email: Peter.Baumhart@usdoj.gov

YAAKOV M. ROTH
Acting Assistant Attorney General
Civil Division

MARCIA BERMAN
JOSEPH E. BORSON, VSB No. 85519
Assistant Directors
Federal Programs Branch
1100 L Street, NW
Washington, D.C. 20005
Tel.: (202) 305-0747
Email: Joseph.Borson@usdoj.gov

Attorneys for Defendants